

This application is submitted in the name of the following inventors:

2

<u>Inventor</u>	<u>Citizenship</u>	<u>Residence City and State</u>
Xiao, Peter	Peoples Republic of China	Fremont, California
Quilice, Jeffrey	United States	Mountain View, CA
Swart, Garrett	United States	Palo Alto, CA
Valente, Luis	Canada	Mountain View, CA

8

The assignee is Network Computer, Inc., having an office at 1000 Bridge Parkway, Redwood Shores, CA 94065.

11

12

Title of the Invention

13

14

Hierarchical Open Security Information Delegation and Acquisition

15

Cross-Reference to Related Applications

16

17

This application claims priority of the following applications:

18

o Application No. 08/770,238, filed December 20, 1996, in the name of inventors Wei Yen and Steven Weinstein, titled "Internet Multiplexer for Broadcast and Other Information", attorney docket NAV-001;

21

1 o Provisional Application Serial No. 60/046,748, filed May 16, 1997, in the name of
2 inventors Luis Valente, Venkatachary Srinivasan, Andreas Atkins and Wei Ling
3 Chu, titled "Client Server Architecture," attorney docket number NAV-008P.

4

5 o Application Serial No. 09/080,571, filed May 18, 1998, in the name of inventors
6 Luis Valente, Venkatachary Srinivasan, Andreas Atkins and Wei Ling Chu, titled
7 "Security Information Acquisition," attorney docket number NCI-008A.

8

9 o Application Serial No. 09/162,650, filed September 29, 1998, in the name of Luis
10 Valente, titled "Security Information Acquisition" attorney docket number NCI-
11 055.

12

13 These applications are referred to herein as the "Incorporated Disclosures,"
14 and are hereby incorporated by reference as if fully set forth herein.

15

16

Background of the Invention

17

18 1. *Field of the Invention*

19

20 This invention relates to computer security.

21

2. *Related Art*

In a data delivery system, data receivers need to know whether they can trust information they receive from senders. This need is increasing due to the growth of data exchanges and business transactions taking place on the Internet over non-secure communication links.

The growing Public Key Infrastructure ("PKI") provides a way for receivers of data to know whether they can trust information they receive from senders. In the PKI, trusted third parties issue digital certificates ("public key certificates") that attest to the authenticity of the binding of a public key to its owner. These trusted third parties are known as certification authorities "CAs", or sometimes are called "public CAs" if their services are available to the public. These digital certificates are created and used using known encryption and decryption security techniques. Verisign, Inc. is an example of a public CA. Senders obtain a certificate from a CA, and include the certificate with the data they wish to send to the receiver. The certificate includes enough information for the receiver to verify that the sender's self-identification is accurate (verification of identity), and that the data was not compromised between the sender and the receiver (validation of contents).

The PKI has the general drawback that digital certificates accepted by the receiver are limited to those from certification authorities that the receiver already trusts.

1 Thus the general problem of providing trust information to the receiver is inherent in the
2 PKI. The trust information required by the receiver can include the identities of trusted
3 senders, for what purpose the senders are trusted, and sufficient information to
4 authenticate messages from the trusted senders.

5

6 For instance, Secure Socket Layer ("SSL") is a widely adopted protocol that
7 is used within the PKI for authentication and encryption. To authenticate a message, the
8 client must have enough trust information regarding the digital certificate sent by the SSL
9 server ("server certificate")--at a minimum the client must have an authentic copy of the
10 certificate of the CA who issued the SSL server certificate. However, computers,
11 particularly in the consumer market, have limited resources, including limited nonvolatile
12 storage, to store such information.

13

14 A computer administrator must decide which CAs to trust. In the case of
15 personal computers used in homes or small offices, the user may be unsophisticated,
16 lacking in knowledge, or unwilling to make and implement his trust decisions. A
17 common solution is providing a factory-defined set of trust relationships. This makes the
18 security measures transparently available to the user. However it is impractical for
19 inexpensive personal computing devices due to the high cost of nonvolatile memory. In
20 addition this solution provides a static set of trust relationships, and does not provide for
21 updates.

22

1 The Incorporated Disclosures provide a method for a computing device to
2 acquire trust information after it is manufactured. These applications disclose the general
3 approach of using Security Information Objects ("SIOs"), with a single Trusted Security
A 4 Information Provider (or at least a single level of TSIPs) defining the trust relationship for
5 all parties. One drawback of the method disclosed is only the TSIP can issue an SIO.
6 Furthermore, the TSIP must administer all parties's trust information, when the TSIP may
7 only be interested in detailed definition of the trust relationship between the TSIP and its
8 closest business partners. Yet, the TSIP may wish to retain some general control over
9 what other partners can do.

10
11 In addition, complex interrelated business relationships exist and are
12 evolving on the Internet, and it is desirable to design a system that will also provide
13 accountability and enforcement of complex business relationships and rules. An example
14 business hierarchy is shown in FIG. 1, and is discussed in detail in the Detailed
15 Description below. Referring to FIG. 1, using the method disclosed in the Incorporated
16 Disclosures, OEM1 and OEM2 would be indistinguishable to ISP1 and ISP2. However,
17 it may be desired to distinguish between OEM1 and OEM2, for instance so that if ISP1 is
18 a client of OEM1, it can be prevented from subscribing to services of OEM2. Or, so
19 OEM2 cannot steal customers of OEM1.

20
21 Accordingly, it would be advantageous for a security system to provide a
22 way for each business party to dynamically provide trust information to its clients based

1 on its own business and security requirements, while centralized control is maintained
2 where desired. The system would be transparent to the end-user, and would be easy to
3 implement.

4

5 The invention provides a Hierarchical Open Security Information
6 Delegation and Acquisition System which allows secure and dynamic distribution of
7 security information to multiple clients over non-secure channels. It also allows parties
8 to modify the security information, within boundaries that are set by higher-level parties.

9 Such modification can include adding third-party CAs to the list of entities trusted to
10 issue SSL certificates. It provides a technique for each business party to define its own
11 trust relationships with other entities including public CAs, within the parameters that are
12 hierarchically set.

13

14

Summary of the Invention

15

16 The invention provides a method and system for secure data transfer and
17 dynamic definition of trustworthiness of various entities by multiple parties in a hierarchy
18 tree or graph structure. ~~The invention uses digital certificates.~~ Each party in the
19 business hierarchy can control and define various trust information including
20 trustworthiness and delegation authority for the entities it deals with. The ability of a
21 party to redefine or add trust information is controlled by the parties with which it has a
22 relationship that are above it in the hierarchy. Trust vectors and delegation vectors are
used to store this information. Each party can add trusted third parties to a security

~~A~~ 1 object without compromising the integrity of security objects already issued. ~~A sequence~~
~~A~~ 2 ~~of security objects including digital certificates can be modified without compromising~~
~~A~~ 3 ~~the original digital certificates in those security objects~~

Brief Description of the Drawings

FIG. 1 shows an example business hierarchy.

FIG. 2 shows the general format of an X509 version 3 certificate.

FIG. 3 shows a schematic of root certificate chaining.

FIG. 4 shows a sample Root Security Information Object for an OEM.

FIG. 5 shows sample values given to bits in ^{a trust/delegation} the trust-delegation vector.

FIG. 6 shows a schematic of how an HSIO chain of RSIOs is linked.

FIG. 7 shows a process flow diagram for a client to validate a Hierarchical Security Information Object.

FIG. 8 shows a process flow diagram whereby an SSL server certificate can be authenticated.

Detailed Description of the Preferred Embodiment

In the following description, a preferred embodiment of the invention is described with regard to preferred process steps and data structures. Those skilled in the art would recognize after perusal of this application that embodiments of the invention can be implemented using one or more general purpose processors or special purpose

1 processors or other circuits adapted to particular process steps and data structures
2 described herein, and that implementation of the process steps and data structures
3 described herein would not require undue experimentation or further invention.
4

5 Alternative embodiments may use other and further forms of authentication
6 and certification, using other forms of cryptography either in addition to or instead of
7 public key cryptography, and are within the scope and spirit of the invention.
8

9 Inventions disclosed herein can be used in conjunction with inventions
10 disclosed in the Incorporated Disclosures, referenced previously.
11

12 *Overview of the Invention*

13
14 The invention provides a secure and dynamic way of distributing trust
15 information from a centralized authority to parties in a hierarchy that have a relationship
16 with it. Among other things, it provides client with enough information to identify
17 trusted SSL servers and authenticate messages from them. It allows each party to define
18 its own trust relationship with the other business parties in the hierarchy and with other
19 entities, including public CAs, within boundaries that are set hierarchically.
20

21 The invention provides a way for the hierarchical structure of business
22 relationships to be incorporated into a security system. The party that is directly above

1 another party in the hierarchy has control over the security information of the lower
2 party--including what kind of third-party entities can be added by the lower party.

3

4 A root certificate of the top-level entity in the hierarchy, the Software
5 Provider ("SP") in the preferred embodiment, is preferably stored in non-volatile memory
6 of a computing device at the time of manufacture. Because subsequent SP root
7 certificates are chained together as described in the Incorporated Disclosures, the
8 computing device can verify any later SP root certificate by chaining back to the one
9 stored in its non-volatile memory. (Or, it can verify by chaining back to a more recent SP
10 root certificate it has stored locally subsequent to time of manufacture.)

11

12 Each of the other parties provides its own root certificate to the party
13 directly above it in the hierarchy. The higher party includes a fingerprint of the lower
14 party's root certificate in a digital object, called the Root Security Information Object
A 15 (RSIO). ~~This allows a path to be verified through the hierarchy, by matching a lower~~
A 16 ~~party to its root certificate fingerprint.~~

17

18 Each party can define detailed trust information, including additional
19 trusted third-party public CAs. Each party generates its own RSIO, which it digitally
20 signs and passes to the next higher party in the tree. RSIOs are the basic source of trust
21 information.

22

1 For any party in the hierarchy, a path can be traced back to the top level
2 party. Each party in the path has an RSIO. When the RSIOs are chained together, that
3 object is called a Hierarchical Security Information Object (HSIO). The RSIOs of the
4 parties (chained into an HSIO) are able to authenticate by tracing an unbroken path of
5 authentication all the way back to the top of the tree, i.e. the Software Provider in the
6 preferred embodiment. Because the SP's root certificate is locally available to all other
7 parties, it can verify the SP's RSIO and each subsequent RSIO can also be verified, given
8 the structure of the RSIOs, as described below.

9 10 *Definitions*

11
12 A "digital certificate" is a non-forgable, tamper-proof electronic document
13 that binds an entity's identity to its public key, as is known in the art of public key
14 cryptography. Public key cryptography is discussed in the Incorporated Disclosures.

1
2 A "root certificate" is a self-signed and self-authenticating digital
3 certificate.

4
5 An entity's "fingerprint" or "signature" is unique data that another entity can
6 recognize as genuine but cannot duplicate. It can function as a person's fingerprint or
7 signature functions in everyday life. In the preferred embodiment, an entity's fingerprint
8 is a SHA-1 hash of its X.509 version 3 certificate.

9
10 A "client" is any computing device that participates in the system, including
11 a classical end-user of a conventional network. Examples of a client are a conventional
12 personal computer or workstation, personal digital assistant, a set-top box, cellular
13 telephone, or digital pager. In discussions of the preferred embodiment the term "client"
14 refers to a set-top box used by a customer of an ISP which could be, for instance, a cable
15 TV service.

16
17 A "party" is one of the entities that is authorized to issue RSIOs.

18
19 *Business Scenario in the Preferred Embodiment*

1 For clarity, the invention is described as applied to a business model in the
2 consumer market, as described below, with the hierarchy having three levels. A sample
3 business hierarchy is shown in FIG. 1.
4

5 In the preferred embodiment, the party at the top of the hierarchy is the
6 Software Provider (SP). It provides software that runs on servers and clients of a web-
7 based TV system.
8

9 The SP has a business contract with one or more Original Equipment
10 Manufacturers ("OEMs"), for the OEM to manufacture and distribute client and server
11 devices that use SP's software. The OEM is the owner of the hardware (servers and
12 clients that run SP's software) used by the lower levels. The OEM is a large national
13 cable TV company that broadcasts shows. The OEM is the middle level of the hierarchy.
14

15 The OEM contracts with one or more Internet Service Providers ("ISPs").
16 The ISP provides service to individual customers. The ISP also provides its customers
17 with OEM client computers running SP software. The ISP is a small local cable
18 company. The hierarchy can assume many shapes. For example, an ISP may contract
19 with several OEMs, or an OEM may contract with several ISPs.
20

21 The invention can be practiced with many other business models. The top-
22 level entity need not be a software provider and need not be affiliated with web-based

1 TV. It can be any entity requiring computer security, including a financial institution, an
2 insurance company, a retail store, a government agency, etc. Likewise, the lower-level
3 entities, if any, can be any entities having a business relationship with the other entities.
4 Currently in the cable television business, it is common for an OEM to also function as
5 the ISP. The business model can have fewer or more than three levels.

6

7 *Root Certificates*

8

9 Each party in the hierarchy provides a root certificate. The root certificate
10 is preferably in X509 version 3 format. A schematic depiction of this format is shown in
11 FIG. 2. Preferably a period of time for which the certificate is valid is stored in the root
12 certificate in the field that is labeled Period of Validity in FIG. 2. (A party's root
13 certificate is provided to the party immediately above it in the hierarchy. This higher
14 party incorporates the root certificate into the as described below.)

15

16 There are three types of root certificates in the preferred embodiment: SP
17 root certificate, OEM root certificate, and ISP root certificate.

18

19 Chaining of SP Root Certificate

20

21 Being the top authority, the SP root certificates are chained together as
22 described in the Incorporated Disclosures. Using this locally stored root certificate,

1 subsequent chained SP root certificates can be verified and validated, as described in the
 2 Incorporated Disclosures. Briefly, root certificate chaining is accomplished by placing,
 3 in the current certificate, a digest--obtained by means of a one-way secure hash function--
 4 of the public key of the next key pair, i.e. the key pair which will replace the current key
 5 pair when the current certificate expires. FIG. 3 illustrates root certificate chaining.

6
 7 Revocation of the root certificate is accomplished.
 8

9 At the time of manufacture, the most recent and valid root certificate for the
 10 SP is stored in nonvolatile memory of the computing device. When an updated SP root
 11 certificate is received, the computing device stores this most recent root certificate.
 12 (Thus, a later SP root certificate need only be verified to the most recent root certificate
 13 that the computing device has previously stored, which saves time.) However, if the
 14 client system reverts to its initial operating state (for instance because of a system
 15 malfunction resulting in the loss of all data in writable storage), the client will always be
 16 capable of verifying a later root certificate using the root certificate that is stored in the
 17 computing device's nonvolatile memory at the time of manufacture.

18 19 OEM and ISP Root Certificates: self-signed and self-authenticating

20
 21 The root certificates of lower level entities (OEM and ISP root certificates
 22 in the preferred embodiment) are just like any public CA certificates: they are self-signed

1 and self-authenticating as known in the art of cryptography. They are not chained
 2 together. To renew or revoke such a root certificate, the certificate is ^{reissued} with new key pairs ^{A2}

3 *Root Security Information Object and Hierarchical Security Information Object*

4
 5 Each party (SP, OEM, ISP) generates its own root security information
 6
 7 object (RSIO). A sample RSIO for an OEM is shown in FIG. 4. The RSIO is digitally
 8 signed by the entity (preferably, by the entity's current root key pair), and preferably
 9 contains a timestamp.

10
 11
 12 The OEM's RSIO and the ISP's RSIO each contains its current active root
 13 certificate. The SP's RSIO preferably contains the SP's entire root certificate chain. That
 14 is, referring to FIG. 4 (which shows a sample OEM RSIO), for an SP RSIO instead of
 15 merely having the root certificate for the SP, the entire chain of root certificates for the
 16 SP is included.

17
 18 A party's RSIO preferably contains an entry for each entity directly below
 19 the party in the hierarchy and can also include a list of the third party CAs that the party
 20 trusts. Each trusted entity (preferably either an OEM, ISP, or third party CA) has an
 21 entry in the RSIO. Each entity is identified by its fingerprint (to save space).

1 The trust information for the each trusted entity is given in the RSIO, and is
 2 preferably implemented by a vector of bits. The delegation information for each trusted
 3 entity is given, and is preferably implemented by a vector of bits.

4

5 Trust Vector and Delegation Vector

6

7 Each entity has associated with it a trust vector. Each bit in the trust vector
 8 designates a role the entity may play. Preferably, some bits in the trust vector indicate
 9 things the entity may do. ^{trust/delegation} A sample ~~trust and delegation~~ vector is shown in FIG. 5. For
 10 example, bit 0 may indicate that the entity is a CA trusted to issue certificates for SSL
 11 clients, and bit 1 may indicate that the entity is a CA trusted to issue certificates for SSL
 12 servers. There may be different grades of SSL servers governed by different bits.

13

14 The trust bits can also indicate what role a Public CA can play. For
 15 example, some Public CAs may only be trusted to issue certificates for low-security
 16 applications such as personal email, whereas other Public CAs may be trusted to issue
 17 certificates for high-security application such as securities trading or electronic funds
 18 transfer.

19

20 Other bits in the trust vector identify the entity as belonging to a certain
 21 class, which is trusted to do certain acts. For instance, bit 2 may indicate that the entity is
 22 an OEM (and thus trusted to issue OEM RSIOs) and bit 3 may indicate that the entity is

1 an ISP (and thus trusted to issue ISP RSIOs. Other bits may indicate the entity is one of
2 SP's special business partners such an SP system software publisher, which is trusted to
3 do certain acts.

4

5 Preferably, each trusted Entity listed in the RSIO has associated with it a
6 delegation vector. Preferably, each bit in the delegation vector designates whether the
7 corresponding trust vector bit may be turned on by the entity next lowest in the RSIO
8 hierarchy. For instance, the delegation vector in the RSIO for a specific OEM indicates
9 what bits ISPs of that OEM may turn on. This has the effect that an ISP may reduce the
10 trust roles the OEM has assigned an entity (by turning off a trust bit) but may not enlarge
11 the trust roles the OEM has assigned to an entity in the RSIO.

12

13 In addition to enabling the OEM to retain control of the changes that an
14 ISP may make, the delegation vector enables the SP to define what authority the OEM or
15 any lower level party has. Thus, the SP can control to some extent what authority all
16 other parties have by being able to prohibit lower entities authority to take certain actions
17 by turning off the delegation vector bit for that action.

18

19 *Chaining of RSIOs*

20

21 The RSIO for an entity contains the fingerprints of its children in the
22 hierarchy. The fingerprint is preferably a hash of the root certificate. That is, the OEM's

1 RSIO contains a hash of the ISP's root certificate, and the SP's RSIO contains a hash of
 2 the OEM's root certificate.

3

4 A chain of RSIO's from the SP's RSIO to OEM's RSIO to ISP's RSIO forms
 5 a Hierarchical Security Information Object. Preferably the chain is formed using the
 6 fingerprint of the root certificate of the next entity in the chain as the link, as shown
 7 schematically in FIG. 6. For instance, the SP RSIO can be linked to OEM1's RSIO by
 8 matching OEM1's fingerprint in the SP's RSIO to the OEM1 identification in OEM1's

9 RSIO. *A31*

11 *HSIO Validation*

13 In the preferred embodiment, the client obtains updated trust information
 14 via an HSIO. Before the client relies on the trust information in the HSIO, it must check
 15 that the HSIO is genuine and has not been tampered with. An HSIO is a chain of RSIO's
 16 from the client back to the SP. In the preferred embodiment, for a client of ISP1, that is
 17 an ISP of OEM1, the RSIO chain will consist of SP's RSIO--->OEM1's RSIO--->ISP1's
 18 RSIO.

19

20 The client can validate the HSIO by the following procedure set out in FIG.

21 7. First check the validity date of the ISP RSIO against the current date. If it is a valid
 22 date, then verify the ISP's RSIO by verifying its signature using the ISP root certificate

1 which is in the ISP RSIO. Check that the ISP fingerprint (hash of its root certificate) is
2 contained in the OEM's RSIO. Check the validity date of the OEM's RSIO, and verify
3 the OEM signature in the OEM RSIO. Check that the OEM fingerprint (hash of its root
4 certificate) is contained in the SP's RSIO. Validate the SP's RSIO by the procedure
5 described in the above and in the Incorporated Disclosures

6

7 If the HSIO passes the checks set out in the previous paragraph, it is a valid
8 and genuine HSIO.

9

10 *Update of HSIO*

11

12 Preferably, the ISP generates new updated HSIOs, because it is the lowest
13 level in the hierarchy, interacting directly with clients. (However, updating of HSIOs can
14 be done by another party.) To generate a new HSIO for a given chain, the ISP needs the
15 current RSIOs of the SP, OEM, and its own RSIO.

16

17 Preferably, the client periodically sends the latest timestamp of the three
18 RSIOs in the HSIO (RSIO chain) to the ISP so that the ISP can determine whether a new
19 HSIO should be sent.

20

1 Events that trigger generation of a new HSIO are the issuance of a new root
 2 certificate by any link in the ~~client~~ ^{client}-ISP-OEM-SP chain, and when the trust information in
 3 any of the RSIOs has changed.

4
 5 *Example: Verification of a non-partner SSL server*

6
 7 An example use of the invention is set forth here. The SSL protocol is
 8 widely used. It may often be desirable for a client to be able to do a transaction with a
 9 computer using SSL that is not one of the SP's business partners. For example, a client
 10 (cable TV customer) that wants to purchase products over a web-based TV application
 11 may need to exchange information with a financial institution SSL server.

12
 13 The client will receive a server certificate, either signed by a CA or else
 14 self-signed, from the third-party server. Suppose server certificate is signed by Verisign
 15 as a public CA. The client must determine whether this CA is trusted to issue a server
 16 certificate.

17
 18 In the preferred embodiment, the ISP is delegated authority to designate
 19 trusted SSL servers and to designate CAs trusted to sign SSL server certificates (In
 20 actual application any specific ISP may or may not have such authority depending on
 21 how higher level entities have delegated authority. To check whether an ISP has
 22 authority to designate CAs trusted to sign SSL certificates, the ^{trust/delegation} ~~trust-delegation~~ vector of

1 the OEM RSIO entry for this ISP would be checked.) In the preferred embodiment, the
2 ISP having authority to designate CAs trusted to do so, the client checks the ISP RSIO to
3 see if Verisign is included as a CA trusted to sign SSL server certificates. (Instead of a
4 CA signing the server certificate, the server certificate may be self-signed, e.g. by
5 Citibank. In such a case, the client checks the ISP RSIO to see whether Citibank is a
6 trusted SSL server.)

7

8 If the CA signing the server certificate (Verisign in our example) is not
9 authorized to do so in the ISP RSIO, then the client checks the OEM RSIO to see if
10 Verisign is included as a CA trusted to sign SSL server certificates. (Or, if instead of CA
11 such as Verisign signing, the server certificate is self-signed, e.g. by Citibank, the client
12 checks the OEM RSIO to see that Citibank is a trusted SSL server.)

13

14 If no authorization is found in the ISP RSIO or the OEM RSIO, then the SP
15 RSIO is similarly checked. If this check fails, then the client cannot do a transaction with
16 this SSL server.

17

18 If authorization is found in any of the RSIOs in the HSIO, then the standard
19 SSL handshake protocol proceeds.

20

21 *Example: Step-Up Encryption*

22

1 Using strong encryption internationally is strictly regulated by the U.S.
2 government. However, a trust bit can be designated to control whether a party is not
3 trusted to use strong encryption. Preferably, this trust bit would be turned off in the SP
4 RSIO for computing devices where strong encryption is allowed. The respective
5 delegation bit would also be turned off, so that lower level entities could not enable
6 strong encryption.

7

8 *Alternative Embodiments*

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2